



+

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED	DATE 05-11-2011 BY 60322 UCBAW
--	--------------------------------

## Attorney Docket No.

*First Inventor or Application Identifier*

REUSEN BAHAN

Title

METHOD AND SYSTEM FOR PREVENTION OF PIRACY OF A GIVEN SOFTWARE APPLICATION VIA A COMMUNICATIONS NETWORK

Express Mail Label No.

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

ADDRESS TO:

*See MPEP chapter 600 concerning utility patent application contents.*

Assistant Commissioner for Patents  
Box Patent Application  
Washington, DC 20231

1. ☒ \* Fee Transmittal Form (e.g., PTO/SB/17)  
(Submit an original and a duplicate for fee processing)
2. ☒ Specification [Total Pages 28]  
(preferred arrangement set forth below)
- Descriptive title of the Invention
  - Cross References to Related Applications
  - Statement Regarding Fed sponsored R & D
  - Reference to Microfiche Appendix
  - Background of the Invention
  - Brief Summary of the Invention
  - Brief Description of the Drawings (if filed)
  - Detailed Description
  - Claim(s)
  - Abstract of the Disclosure
3. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets 2]
4. Oath or Declaration [Total Pages ]
- a. ☒ Newly executed (original or copy)
  - b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d))  
(for continuation/divisional with Box 16 completed)
  - i. ☐ DELETION OF INVENTOR(S)  
Signed statement attached deleting inventor(s) named in the prior application,  
see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

5. ☐ Microfiche Computer Program (*Appendix*)
6. Nucleotide and/or Amino Acid Sequence Submission  
(if applicable, all necessary)
- a. ☐ Computer Readable Copy
- b. ☐ Paper Copy (identical to computer copy)
- c. ☐ Statement verifying identity of above copies

### ACCOMPANYING APPLICATION PARTS

7. ☒ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. §3.73(b) Statement ☐ Power of Attorney  
(when there is an assignee)
9. ☐ English Translation Document (if applicable)
10. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☐ Return Receipt Postcard (MPEP 503)  
(Should be specifically itemized)
13. ☒ \* Small Entity Statement(s) ☐ Statement filed in prior application, Status still proper and desired  
(PTO/SB/09-12)
14. ☐ Certified Copy of Priority Document(s)  
(if foreign priority is claimed)
15. ☐ Other: .....

\* NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment
- |                          |              |                          |            |                          |                            |                                      |
|--------------------------|--------------|--------------------------|------------|--------------------------|----------------------------|--------------------------------------|
| <input type="checkbox"/> | Continuation | <input type="checkbox"/> | Divisional | <input type="checkbox"/> | Continuation-in-part (CIP) | of prior application No. _____/_____ |
|--------------------------|--------------|--------------------------|------------|--------------------------|----------------------------|--------------------------------------|

Prior application information. Examiner \_\_\_\_\_ Group / Art Unit. \_\_\_\_\_

**For CONTINUATION or DIVISIONAL APPS only:** The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

## 17. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label*

or ☐ Correspondence address below

(Insert Customer No. or Attach bar code label here)

Name \_\_\_\_\_

REVISEN BAHAR

*Address*

23708 WELBY WAY

City

WEST HILLS

State

CA

*Zip Code*

91307

Country

USA

*Telephone*

(818) 884-3160

Fax:

(818) 346-9564

Name (Print/Type)

KEUTZEN BAHAR

Registration No. (Attorney/Agent)

*Signature*

孙 恩

Date \_\_\_\_\_

6/13/2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

**STATEMENT CLAIMING SMALL ENTITY STATUS  
(37 CFR 1.9(f) & 1.27(b))--INDEPENDENT INVENTOR**

Docket Number (Optional)

Applicant, Patentee, or Identifier: REUBEN BAHAR

Application or Patent No.: \_\_\_\_\_

Filed or Issued: \_\_\_\_\_

Title: METHOD AND SYSTEM FOR PREVENTION OF PIRACY OF A GIVEN SOFTWARE APPLICATION  
VIA A COMMUNICATIONS NETWORK.

As a below named inventor, I hereby state that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees to the Patent and Trademark Office described in:

- ☒ the specification filed herewith with title as listed above.  
☐ the application identified above.  
☐ the patent identified above.

I have not assigned, granted, conveyed, or licensed, and am under no obligation under contract or law to assign, grant, convey, or license, any rights in the invention to any person who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern, or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

- ☒ No such person, concern, or organization exists.  
☐ Each such person, concern, or organization is listed below.

Separate statements are required from each named person, concern, or organization having rights to the invention stating their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

REUBEN BAHAR  
NAME OF INVENTOR

NAME OF INVENTOR

NAME OF INVENTOR

[Signature]  
Signature of inventor

Signature of inventor

Signature of inventor

6/13/2000  
Date

Date

Date



1 illegal copies of a software application and distributing them in mass  
2 quantities for drastically reduced prices.

3 Due to the availability and low cost of sophisticated computer  
4 equipment such as the CD Write / Re-Write drive, software piracy has  
5 become a much greater concern over the current years. Today, virtually  
6 everyone can get access to such equipment and distribute CD based copies  
7 of software applications to whomever they please. Mass distribution of  
8 pirated software not only deprives the software manufacturer of their  
9 deserved earnings, but also allows other software pirates to pirate  
10 unlicensed copies of that application and propound the damage  
11 exponentially. As such, piracy has often resulted in inflated software  
12 prices and irreparable damage to software companies.

13 In efforts to combat the problems of software piracy, many software  
14 companies have enabled various preventative measures. Some of these  
15 include software access codes, activation plugs (i.e. memo hasp),  
16 registration, and even costly technical support services. Although  
17 somewhat effective, these measures have often been defeated with relative  
18 ease and little or no expense. For example, software access codes which  
19 must be entered to gain access to the software, are disclosed with the  
20 software package and are thus, easily copied and distributed to  
21 unlicensed users. Activation plugs, such as the ones which attach to the  
22 PC's parallel port, have also been easily duplicated by various  
23 manufacturers who illegally sell them on the black market. Furthermore,  
24 while registration of the software would inform the manufacturer of all  
25 users (licensed and unlicensed), pirates rarely do it given the absence  
26 of a compelling motivation to do so. Lastly, technical support groups

are likewise, rarely used by pirators given their reluctance to disclose their illegal use of the software. As shown by these and other ineffective measures, it would be advantageous for a software manufacturer to control the functionality of a given software application in relation to each of its identified users.

#### BRIEF SUMMARY OF THE INVENTION

It is the object of the present invention to provide a reliable and effective method and system for preventing piracy of a given software application over a communications network, whereby the software application will not function unless activated by a remote service provider.

It is further the object of the present invention to provide a method and system for identifying each separate user of a given software application who installs and intends to effectively utilize the given software application.

It is further the object of the present invention to provide a method and system for associating user data to archived data accessible by the remote service provider, in order to determine if the user is a pirator of the software application.

The present invention is for a method and system for preventing piracy of individual software applications. A remote service system, controlled by a remote service provider, storably receives user data that is transmitted by a user of a given software application. Upon receiving the user data, the remote service system associates it to stored archive data which is accessible to the remote service provider. If it is

1 determined that the user is not a pirator of the software, the remote  
2 service system will transmit service data which will activate the  
3 software and allow the user to utilize its full functionality. In this  
4 manner, the remote service provider can limit software piracy as only  
5 legitimate users of the software will be given the service data needed to  
6 activate the software.

#### 8 BRIEF DESCRIPTION OF THE DRAWINGS

9 FIG. 1 is an overview diagram pictorially illustrating the flow of  
10 information that occurs between a user of a given software application  
11 and the remote service system in the method and system for prevention of  
12 software piracy according to the present invention.

13 FIG. 2 is a block flowchart of the information flow that occurs in  
14 the method and system for prevention of software piracy according to the  
15 present invention.

#### 17 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

18 In reference now to the drawings, FIGS. 1 and 2 show the information  
19 flow that occurs in a method and system (hereinafter "method"), indicated  
20 at reference character 100 in FIG. 1, for prevention of piracy of a given  
21 software application via a communications network, such as the Internet  
22 8. Both FIGS. 1 and 2 illustrate the process by which a user would  
23 attempt to activate a given software application.

24 As shown in FIG. 1, the user 1 successfully installs a given  
25 software application 5 (hereinafter "software"), on the data storage  
26 element 4 of their user system 2. The user system 2 is generally defined

as the user's computer terminal, which typically consists of a central processing unit (CPU) (not shown), data storage element 4, element for storablely receiving transmitted data 3, element for transmitting data 6, and a monitor and keyboard. While the software 5 may utilize various anti-piracy measures, two, which will later be discussed in detail, are especially worth noting in relation to this invention. The first measure is a program code sequence that identifies the specific software 5 (hereinafter "identification code"), while the second is an additional program code sequence that would be needed to activate the software 5 (hereinafter "activation code"). It is preferred that transmission of both of these code sequences, between the user 1 and remote service system 9, would be accomplished over the Internet 8. As used in this invention, a user can be an individual entity or collaborate entity, such as a business, family, or even friends, who legitimately acquired a license and/or right to use the given software 5. Furthermore, the remote service system 9 can be the software manufacturer or an independent company, working in conjunction with the software manufacturer, which will operate to prevent software piracy as noted in this invention.

Upon an initial attempt to access the installed software 5, the user 1 will be informed that the software 5 will require online activation before it can be operational. Online activation will render the given software 5 operational, subject to receiving the activation code from the remote service system 9. This requires that the software 5 be designed wherein it is either partially or completely dysfunctional prior to receiving the activation code, as will be discussed below. By

1 connecting to the remote service system 9 through the Internet 8, a user,  
2 who is not pirating the software 5, will be able to have the software 5  
3 activated online. Although the Internet 8 is used exclusively when  
4 referencing a communications network, the present invention is intended  
5 to include all forms of communications network environments known to one  
6 skilled in the relevant art. Thus, method 100 is equally applicable to  
7 all interconnected computer systems capable of transmitting and receiving  
8 data, preferably digital data, which allow users of the network to  
9 communicate. In this regard, a communications network includes, but is  
10 not limited to, all telecommunications networks such as the Internet,  
11 i.e. the World Wide Web and BBS systems, hardwire telephony, wireless  
12 networks including cellular and PCS systems, satellite networks, etc.  
13 Furthermore, communications networks include localized and regional  
14 networks such as intranets and local area network (LAN) systems which  
15 interconnect a relatively few number of user systems or terminals,  
16 typically by means of a centralized server.

17 Once the user 1 establishes an online connection to the remote  
18 service provider 9, they will enter and transmit user data 7, by element  
19 for transmitting user data 6, to the remote service system 9 over the  
20 internet 8. The user data 7 would subsequently, be received by the  
21 remote service system 9 via element for storably receiving user data 10,  
22 and stored in the data storage element 12 of the remote service system 9.  
23 Although the transfer of user data 7 to the remote service system 9 would  
24 preferably be initiated by the user 1, this need not always be the case.  
25 Once the user 1 connects to the remote service system 9 via the



Internet 8, the user data 7 may be automatically detected by element for detecting user data 11 of the remote service system 9. In this case, the detected user data 7 will likewise be received by the remote service system 9 via element for storably receiving user data 10, and subsequently stored by the data storage element 12 of the remote service system 9. It is notable that the term user data is defined and understood herein and in all the claims to mean any information originating from and/or available to the user of the software 5. This includes, but is not limited to personal identification information such as user name, address, location, phone number, etc. Additionally, user data 7 may consist of any information relating to the software 5 which identifies and distinguishes it from other "same type" or distinct software applications. This can include, but is not limited to information such as an "identification code" (as noted earlier), a product serial number, name, and/or version number.

It is worthy to mention that the software 5 should preferably contain an identification code, which is a program code sequence comprised of alphanumeric characters, that would serve to identify each individual software application. Given its function, the identification code may also be synonymous to a product's distinct serial number. Preferably, the identification code will be unique to each software application sold and disclosed to both the user 1 and remote service system 9. The advantage of a unique identification code is that it will allow the remote service system 9 to recognize and keep track of each software application sold. Although the identification code could consist of an elongated alphanumeric code sequence, such as a "program

1 file(s)", it is preferred that it consist of a short code sequence of  
2 alphanumeric characters, e.g. XJR-U89K-RJ2P1. A short identification  
3 code sequence will allow the software 5 to be simply and easily  
4 identified. It should finally be noted that user data 7 may also refer  
5 to information identifying the user system 2 such as serial and model  
6 number as well as the type, function, and performance of the various  
7 system hardware components.

8 After receiving and storing the user data 7, the remote service  
9 system 9 will process the user data 7 via element for processing user  
10 data 13. Element for processing user data 13 may be, but is not limited  
11 to software, hardware device(s), or a combination of these two, which  
12 would allow for processing of the user data, as noted in this invention.  
13 Additionally, element for processing user data 13 may likewise include  
14 the remote service system's personnel staff who would be able to manually  
15 initiate processing of the user data, as noted in this invention.

16 Processing of the user data may include, but is not limited to an  
17 "archiving" event wherein a wide range of information that is received by  
18 or made available to the remote service system 9 is sorted, arranged, and  
19 organized into retrievable data files. Archived data stored in the data  
20 storage element 12 of the remote service system 9 may consist of, but is  
21 not limited to, a mass assortment of receivably stored user data (e.g.  
22 "identification codes"), service data (discussed below), and promotions,  
23 etc. Here, the archived data would relate to distinct users, various  
24 software applications, and potential advertisements; all of which may  
25 exist independently of one another. Second, archived data may also  
26 consist of information indicating the amount of user online activation

1 attempts recorded for each identified software 5. Finally, archived data  
2 would include all other information that would be of use to the remote  
3 service system 9 in preventing piracy of a given software application, as  
4 noted in this invention.

5 Processing of the user data 7 may also consist of an "associating"  
6 event wherein the currently transmitted user data 7 is compared to  
7 archived data contained in the data storage element 12 of the remote  
8 service system 9. It is important to note that "associating" the  
9 currently transmitted user data 7 to archived data will allow the remote  
10 service system 9 to determine if the user 7 is attempting to activate a  
11 pirated version of the software 5. Here, the "product identification  
12 code" of software 5, along with other user data 7 currently being  
13 received from the user system 2, will be compared to existing archived  
14 data. If the archived data informs that the software 5 is legally  
15 registered to a completely distinct user, such may indicate that the user  
16 currently online is trying to activate a pirated version of the  
17 software 5. This result will occur if the archived data referencing the  
18 software 5 does not match the user data 7 currently being transmitted by  
19 the user system 2, and/or if the archived data indicates that there has  
20 been repeated and numerous attempts to activate the same software 5.

21 Multiple online activation attempts of the same software 5,  
22 regardless if such attempts are by distinct or the same users would  
23 naturally indicate that the software 5 was pirated and distributed to a  
24 multitude of different users. In this situation, the remote service  
25 provider may contact the registered user(s) to investigate into potential  
26 piracy. Additionally, the remote service system 9 may blacklist the

1 specific software 5, as referenced by its identification code.  
2 Blacklisting of a given software application would mean that the  
3 identified software would be prohibited from receiving any future  
4 activation codes from the remote service system 9. For all intensive  
5 purposes, such an event would render the identified software void and  
6 permanently dysfunctional. This is because the software, as sold to the  
7 user, would need the activation code in order to function. Absent this  
8 code, the identified software would be inoperative and no longer subject  
9 to piracy.

10 When it is determined by the remote service system 9 that the user 2  
11 is not a pirator of the software 5, service data, such as the activation  
12 code 17, may be transmitted to the user system 2. Here, the software 5  
13 and/or the user system 2 would be responsive to the service data. As  
14 used in this invention, service data is defined and understood herein and  
15 in all the claims to mean any data that the remote service system 9 may  
16 legitimately transmit to the user system 2 during the online activation  
17 process for the software 5. Service data 16 may include, but is not  
18 limited to instructions, promotional messages, and an activation code(s).  
19 The instructions may guide the user 1 through the steps for activating  
20 the software 5, while a promotional message program code sequence may  
21 offer and display a particular product or service for sale. The  
22 activation code 17, as noted earlier, is a program code sequence that  
23 will serve to activate each individual software application, which absent  
24 the activation code 17, would be dysfunctional. The activation code may  
25 either be unique to each individual software 5 sold (hereinafter "unique  
26 activation code") or unique to a group of software (hereinafter "common

1 activation code") that relate to a common software program, manufacturer,  
2 brand name, or version, etc. Of the two, the preferred embodiment would  
3 be the "unique activation code" which is unique to each individual  
4 software 5 sold.

5 One of the main advantages of using a unique activation code is the  
6 drastic curtailment of software piracy. Here, each software 5 will be  
7 designed wherein it is responsive to a distinct activation code. As  
8 such, an attempt to pirate distinct software applications would entail a  
9 tedious and time consuming task requiring the hacker to uncover the  
10 activation code of each individual software. Furthermore, a unique  
11 activation code will not allow for the activation of any "general" copy  
12 of the software which would otherwise be responsive to a common  
13 activation code. As an alternative to a unique activation code, a common  
14 activation code would activate all "same type" software applications.  
15 Developing "same type" software to be responsive to a common activation  
16 code may be advantageous given the potential for less confusion and  
17 troubleshooting errors which could arise during the software  
18 manufacturing and online activation stages.

19 It is noteworthy to mention that similar to the identification code,  
20 the activation code may likewise consist of either a long or short  
21 program code sequence. As noted earlier, a short code sequence would  
22 consist of a concise sequence of alphanumeric characters,  
23 e.g. HT3-GY2K-WR0P, while a long code sequence would consist of a small  
24 or large arrangement of alphanumeric data that result in a "program  
25 file(s)". Use of a long code sequence would be the preferred method of  
26 constructing the activation code. This is because a long code sequence

1 (i.e. a program file) would be much harder to replicate than a short code  
2 sequence. Here, the software 5 may be developed wherein it is missing  
3 program files necessary for it to function. Only after these undisclosed  
4 program files (e.g. the activation code) are transmitted from the remote  
5 service system 9 to the user system 2, will the software 5 be functional.

6 An activated software application will be fully operational and  
7 allow the user complete access to it. Although it need not be so, it is  
8 preferred that the activation code 17 remain undisclosed to the user 2.  
9 Here, the need for the activation code will compel the user 2 to register  
10 the software 5 online with the remote service system 9. Furthermore, and  
11 more importantly, having the activation code 17 only known to the remote  
12 service provider and its business affiliates (such as the software  
13 manufacturer) will prevent piracy of the software 5. This is because  
14 users who wish to pirate the software 5 will not be able to replicate the  
15 activation code and distribute it along with a medium (e.g. CD Rom)  
16 containing a copy of the software 5. Given this, it is additionally  
17 preferred that the activation code 17 be designed wherein it is immune to  
18 discovery by computer hackers and sophisticated programmers. The  
19 objective here is to prevent these individuals from "breaking in" to the  
20 software 5 and either re-writing or discovering the undisclosed  
21 activation code. As noted earlier, this may require constructing the  
22 activation code as a long code sequence which results in a program  
23 file(s). Additionally, other measures may include code encryption as  
24 well as any other programming methods known to those skilled in the  
25 relevant technical art.

26 Before a software 5 can be activated, the appropriate service data

1 must be processed and transmitted to the user system 2. Processing of  
2 the service data 16 would require that it be either extracted or  
3 generated from the archived data stored on the data storage element 12 of  
4 the remote service system 9. Extraction or generation of the service  
5 data 16 will be accomplished by element for processing service data 14,  
6 as referenced in Method 100 of FIG. 1. Element for processing service  
7 data 14 may be, but is not limited to software, hardware device(s), or a  
8 combination of the two, which would allow for processing of the service  
9 data, as noted in this invention. Additionally, element for processing  
10 service data 16 may likewise include the remote service system's  
11 personnel staff who would be able to manually initiate processing of the  
12 service data 16, as noted in this invention.

13 Extraction of service data 16 from the archived data entails a  
14 selection process wherein only the appropriate and necessary service data  
15 is singled out from the total archived data and made available for  
16 transmission to the user system 2. Extraction of the service data is  
17 necessary given the multitude of distinct service data information that  
18 may be stored and archived by the remote service system 9. For example,  
19 the activation code "ABC-123", contained in the archived data, would only  
20 be extracted when a user 1 who possesses the specific software  
21 referencing the identification code "ABC-123" attempts to activate it  
22 online. Stated differently, service data containing an activation code  
23 relating to Microsoft Word 2000 would not be extracted for a user trying  
24 to activate a Norton Anti-virus software application. The reason for  
25 this is that different users will require different service data,  
26 depending on the requirements of the specific software that they are

1 attempting to activate.

2 Alternatively, the second embodiment for processing the service  
3 data 16 pertains to an event which causes the service data 16 to be  
4 generated. This event entails a process wherein pre-existing archive  
5 data may be formulated into the appropriate service data upon request  
6 from the remote service system 9. Generation of service data can be  
7 advantageous as this method will permit the remote service system 9 to  
8 manipulate various data components, existing in the archived data, in  
9 order to formulate the service data 16. For example, the remote service  
10 system 9 may combine personal identification information belonging to the  
11 user 1 with promotional data to formulate a personalized advertisement  
12 directed at the user 1. Additionally, the remote service system 9 could  
13 combine user data (such as the directory file location of the user system  
14 2 that contains the installed software 5) with the appropriate activation  
15 code, to formulate a self executing program file which, upon an access  
16 event, would automatically install the service data 16 into the correct  
17 file location of the user system 2. Here, formulation of the service  
18 data may include, but is not limited to a series of calculations,  
19 combinations, and/or sorting out of the appropriate archived data.  
20 Generation of the service data may occur at any time prior to or after  
21 the remote service system 9 determines that the user 1 is not a pirator  
22 of software 5 and is eligible to receive the service data 16.

23 Once the service data 16 is extracted or generated via element for  
24 processing service data 14, the remote service system 9 will transmit it  
25 to the user system 2. Transmission of the service data 16 may be  
26 accomplished in a number of ways. The first two methods involve an event



1 wherein the service data 16 is uploaded into the user system 2, while the  
2 third method requires the user 1 to download the service data 16 into  
3 their user system 2. In the first embodiment for uploading the service  
4 data 16, the remote service system 9 initiates an uploading event in  
5 which the service data is automatically transferred from the remote  
6 service system 9 to the user system 2 wherein it is storablely received via  
7 element for storablely receiving 3 service data 16. In doing this, the  
8 remote service system 9 may find it necessary to determine the  
9 appropriate file directory location of the user system 2 in which to  
10 upload the service data. Determination of this location may be  
11 accomplished by, but is not limited to user 1 disclosure, as transmitted  
12 by the user (e.g. user data), or via an interactive search of the file  
13 directory of user system 2.

14 In the second embodiment for uploading of the service data 16, the  
15 remote service system manually transmits the service data 16 to the user  
16 system 2. Manual transmission of the service data 16 would allow remote  
17 service system personnel to decide when the transfer sequence should be  
18 initiated. Furthermore, manual transmission would enable such personnel  
19 to manually enter and transmit needed service data 16 which may not have  
20 been processed by the element for processing service data 14 of the  
21 remote service system 9. Finally, in the third method for transmitting,  
22 the service data 16 may be made available to the user 1 for them to  
23 download into their user system 2. Here, the remote service system 9  
24 generates the archived data 16 into a file that can be downloaded by the  
25 user 1. The file would contain service data and possibly some elements  
26 of user data. It is preferred (as discussed earlier) that the file

1 contain a self-executing installation program that is triggered upon an  
2 access event by the user. For example, as a result of successful  
3 downloading and accessing of the file, the service data 16 will  
4 automatically be installed into the appropriate file directory of the  
5 user system 2.

6 Following successful upload or installation of the service data 16  
7 (such as the activation code 17) into the user system 2, the software 5  
8 will gain full functionality. Complete activation of the software 5 will  
9 allow the user 1 to freely utilize it to its full potential. Preferably,  
10 the user 1 will never need to go through the online activation process  
11 (as mentioned herein) again unless they attempt to install the software 5  
12 on another user system or re-install it on their current user system 2.

13 Although many different scenarios can arise during the online  
14 activation process of a given software 5, FIG. 2 illustrates, in block  
15 diagram form, one possible "real time" cycle run of the present  
16 invention. Starting from block 18, the user 1 successfully installs a  
17 given software application on their user system 2, at block 19. Upon an  
18 initial access event of the software 5, as shown at block 20, the  
19 software 5, at block 21, will inform the user 1 that online activation is  
20 required in order for it to function. If the user 1 decides to register  
21 the software 5, they must connect online to the appropriate remote  
22 service system 9, as shown at block 22. At this point, the remote  
23 service system 9 may request from the user 1 that they enter and transmit  
24 user data 7 to the remote service system 9, block 23. In addition to  
25 this, the remote service system 9 may also attempt to detect any user  
26 data 7 that can be detected by virtue of the online connection between

1 the user system 2 and remote service system 9, block 24. If the  
2 appropriate and necessary user data 7 is entered and transmitted by the  
3 user 1, block 25, or detected by the remote service system 9, block 26,  
4 then it will be stored and processed by the remotes service system 9 as  
5 indicated at block 27. It should be noted that where the user 1 fails to  
6 provide and transmit the appropriate and necessary user data 7, and/or  
7 the remote service system 9 is unable to detect the appropriate and  
8 necessary user data 7, the cycle will repeat and be taken back to  
9 block 23.

10 The processing of the user data 7 will allow the remote service  
11 system 9 to determine if the user is a pirator of the software 5. If the  
12 remote service system 9 determines that the user 1 is not a pirator, at  
13 block 28, service data 16 will be processed, block 29. At this point,  
14 the remote service system 9 will transmit the service data 16 to the user  
15 system 2, at block 30. Transmission may be accomplished via uploading or  
16 downloading methods as described earlier. After the service data 16 is  
17 storably received by the user system 2, block 31, the software 5 will be  
18 active and fully operational subject to successful activation by the  
19 service data 16, block 32. In the event that the service data 16 was not  
20 properly received by the user system 2, or effective in activating the  
21 software 5, the cycle will repeat, starting from block 18.

22 Finally, it is noteworthy to mention that in the event that the  
23 remote service provider determines that the user 1 is pirating the  
24 software 5, it may refuse to transmit the service data 16, as shown by  
25 block 33. Additionally, it may investigate into the possibility of  
26 piracy, at block 34, as well as blacklist the identified software 5,

1 at block 35.

2 The program code sequence and all other technical aspects required  
3 by this invention are all conventional and known to those skilled in the  
4 art and need not be described in detail herein. Furthermore, the term  
5 "element", as stated in the specification and all the claims herein, may  
6 be construed in the plural tense as would be necessary in regards to each  
7 noted reference made.

8 The present embodiments of this invention are thus to be considered  
9 in all respects as illustrative and not restrictive; the scope of the  
10 invention being indicated by the appended claims rather than by the  
11 foregoing description. All changes which come within the meaning and  
12 range of equivalency of the claims are intended to be embraced therein.

**I CLAIM:**

1. A method of preventing piracy of a given software application via a communications network, said method comprising the steps of:
  - storably receiving user data on data storage element of a remote service system via element, of said remote service system, for storably receiving said user data, said remote service system connected to said communications network and designated to receive said user data;
  - associating said user data to archived data of said remote service system via element, of said remote service system, for processing user data, wherein said association event is initiated to determine whether said user is pirating said software application;
  - selectively transmitting service data to user system via element, of said remote service system, for transmitting said service data when said remote service system determines that said service data should be transmitted, said user system connected to said communications network and designated to storably receive said service data.

1        2.        The method as in Claim 1,

2                wherein said user data is transmitted by said user to  
3                said remote service system via element, of said user system,  
4                for transmitting user data, said user system connected to said  
5                communications network and designated to transmit said user  
6                data.

7        3.        The method as in Claim 2,

8                wherein said user data comprises of at least one program  
9                code sequence that identifies said software application  
10               stored on data storage element of said user system.

11       4.        The method as in Claim 2,

12               wherein said user data includes identity information  
13               relating to said user of said software application.

14       5.        The method as in Claim 2,

15               wherein said user data includes product information  
16               relating to said software application stored on said  
17               data storage element of said user system.

18       6.        The method as in Claim 2,

19               wherein said user data includes system hardware  
20               information relating to said user system.

1        7.        The method as in Claim 1,  
2                wherein said user data is detected by said remote  
3        service system via element, of said remote service system, for  
4        detecting said user data, said remote service system  
5        connected to said communications network and designated  
6        to detect said user data.

7        8.        The method as in Claim 7,  
8                wherein said user data comprises of at least one program  
9        code sequence that identifies said software application stored  
10       on said data storage element of said user system.

11       9.        The method as in Claim 7,  
12                wherein said user data includes identity information  
13       relating to said user of said software application.

14       10.       The method as in Claim 7,  
15                wherein said user data includes product information  
16       relating to said software application stored on said data  
17       storage element of said user system.

18       11.       The method as in Claim 7,  
19                wherein said user data includes system hardware  
20       information relating to said user system.







1     21.     The method as in Claim 1,  
2             wherein the step of transmitting said service data  
3             is a downloading event in which said service data is made  
4             available to said user from said remote service system, said  
5             user being able to download said service data into said user  
6             system via element, of said user system, for storably receiving  
7             said service data.

8     22.     The method as in Claim 1,  
9             wherein, said software application includes a  
10            program code sequence that identifies said software  
11            application stored on said data storage element of said  
12            user system, said software application additionally being  
13            responsive to a second program code sequence that  
14            activates said software application, and which is transmitted  
15            to said user system via said communications network.

1 23. A system for preventing piracy of a given software  
2 application via a communications network, said system  
3 comprising:

4 a user system connected to a communications  
5 network and designated by a user to transmit user  
6 data and storably receive service data, said user system  
7 including computer processor element, data storage element for  
8 storing data, element for transmitting user data, and element  
9 for storably receiving said service data.

10 a remote service system connected to said  
11 communications network and designated by the remote  
12 service provider to storably receive said user data and  
13 selectively transmit said service data, said remote  
14 service system including computer processor element, data  
15 storage element for storing data, element for storably receiving  
16 said user data, element for detecting said user data, element  
17 for processing said user data, element for processing said  
18 service data, and element for transmitting said service data to  
19 said user system.

20 24. The system as in Claim 23,

21 wherein said user data is detected by said remote  
22 service system via element, of said remote service system, for  
23 detecting said user data, said remote service system  
24 connected to said communications network and designated to  
25 detect said user data.

1 25. The system as in Claim 23,

2 wherein said service data is extracted from said  
3 archived data by element for processing said service data.

4 26. The system as in Claim 23,

5 wherein said service data is generated from said  
6 archived data by element for processing said service data.

7 27. The system as in Claim 23,

8 wherein the steps for transmitting said service data  
9 is an uploading event in which said service data is automatically  
10 transferred from said remote service system and storably received  
11 by said user system via element, of said user system, for  
12 storably receiving said service data.

13 28. The system as in Claim 23,

14 wherein the steps for transmitting said service data  
15 is an uploading event in which said service data is manually  
16 transferred from said remote service system and storably received  
17 by said user system via element, of said user system, for  
18 storably receiving said service data.

19

20

21

22

23

1 29. The system as in Claim 23,  
2 wherein the steps for transmitting said service data  
3 is a downloading event in which said service data is made  
4 available to said user from said remote service system, said user  
5 being able to download said service data into said user system  
6 via element, of said user system, for storablely receiving said  
7 service data.

8 30. The system as in Claim 23,  
9 wherein said software application includes a program  
10 code sequence that identifies said software application  
11 stored on said data storage element of said user system,  
12 said software application additionally being responsive to  
13 a second program code sequence that activates said  
14 software application, and which is transmitted to said  
15 user system via a communications network.  
16  
17  
18  
19  
20  
21  
22  
23  
24

## ABSTRACT

A method and system for prevention of piracy of a given software application via a communications network, such as the Internet. A given software application, installed on a user system, will not function until it is activated by a remote service provider. This will require the user to provide the remote service provider with user data, such as the user's personal identity information and the unique software identification code relating to the specific software. User data will then be compared to archived data in order to determine if the user is a pirator of the software. If not a pirator, the remote service provider may transmit undisclosed service data, such as a software activation code, to the user system. Once activated, the software will become fully operational and allow the user complete access to its functions. In this manner, piracy of a given software application can be prevented.



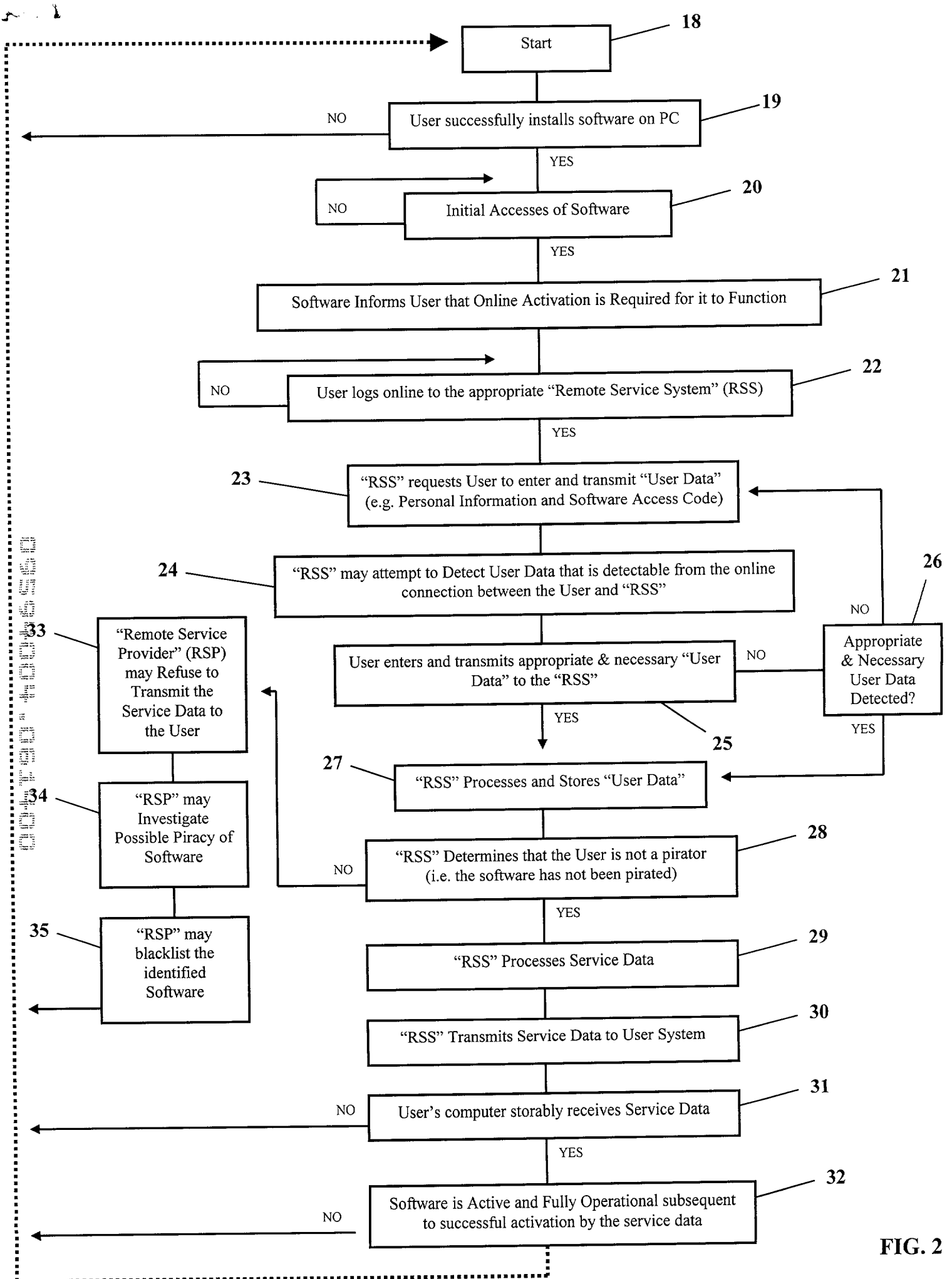


FIG. 2



Please type a plus sign (+) inside this box → ☐

PTO/SB/01 (12-97)  
Approved for use through 9/30/00. OMB 0651-0032  
Patent and Trademark Office, U. S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION</b> <b>(37 CFR 1.63)</b>  <input checked="" type="checkbox"/> Declaration Submitted with Initial Filing    OR <input type="checkbox"/> Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)	<b>Attorney Docket Number</b>	
	<b>First Named Inventor</b>	REUBEN BAHAR
	<b>COMPLETE IF KNOWN</b>	
	<b>Application Number</b>	/
	<b>Filing Date</b>	
	<b>Group Art Unit</b>	
	<b>Examiner Name</b>	

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND SYSTEM FOR PREVENTION OF PIRACY OF A GIVEN SOFTWARE APPLICATION VIA A COMMUNICATIONS NETWORK

the specification of which (Title of the Invention)

☒ is attached hereto  
OR

☐ was filed on (MM/DD/YYYY) as United States Application Number or PCT International

Application Number and was amended on (MM/DD/YYYY) (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box →



PTO/SB/01 (12-97)  
Approved for use through 9/30/00 OMB 0651-0032  
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

## DECLARATION — Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)

☐ Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

☐ Customer Number

OR

☒ Registered practitioner(s) name/registration number listed below

Place Customer  
Number Bar Code  
Label here

Name	Registration Number	Name	Registration Number
REUBEN BAHAR	(INVENTOR)		

☐ Additional registered practitioner(s) named on supplemental Registered Practitioner Information sheet PTO/SB/02C attached hereto

Direct all correspondence to: ☐ Customer Number

or Bar Code Label

OR ☒ Correspondence address below

Name	REUBEN BAHAR				
Address	23708 WELBY WAY				
Address					
City	WEST HILLS	State	CA	ZIP	91307
Country	USA	Telephone	(818) 884-3160	Fax	(818) 346-9564

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any))	Family Name or Surname
REUBEN	BAHAR

Inventor's Signature				Date	6/13/00		
Residence: City	WEST HILLS	State	CA	Country	USA	Citizenship	USA
Post Office Address	23708 WELBY WAY						
Post Office Address							
City	WEST HILLS	State	CA	ZIP	91307	Country	USA

☐ Additional inventors are being named on the \_\_\_\_\_ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto